

REMARKS

Claims 1, 3-25 and 27-32 are pending. Claims 1 and 25 are amended herein.

103 Rejections

Claims 1, 3-9, 11, 13-22, 24-25, 27-30 and 32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Pallman in view of Blum et al. and further in view of Booth. Applicant respectfully submits that Pallman in view of Blum et al. and further in view of Booth does not anticipate or render obvious the embodiments of the present invention as are set forth in Claims 1, 3-9, 11, 13-22, 24-25, 27-30 and 32.

The Examiner is respectfully directed to Claim 1 which is presented below in its entirety for the Examiner's convenience:

1. (currently amended) A method for a local computer system to control a remote system over the Internet, comprising the steps of:
 initiating a log-in procedure by the local computer system;
 verifying whether a user is authorized to access the remote system by accessing a server that is remote from the local computer system;
 accepting a command from an authorized user by the local computer system;
 executing the command through File Transfer Protocol to perform a function on the remote system;
 issuing the command through the web browser on the local computer system;
 transmitting the command over the Internet as Hypertext Transfer Protocol without File Transfer Protocol components;

processing the Hypertext Transfer Protocol command into a File Transfer Protocol command using the server that is remote from the local computer system; and forwarding the file Transfer Protocol command to the remote system. (emphasis added)

Claims 15 and 25 recite limitations similar to those that are recited in Claim 1. Claims 3-9, 11, 13 and 14 depend from independent Claim 1, Claims 16-22 and 24 depend from independent Claim 15, and Claims 27-30 and 32 depend from independent Claim 25 and recite additional limitations of the present claimed invention.

Pallman does not anticipate or render obvious a method for controlling a remote system over the Internet by executing a command through File Transfer Protocol including the steps of “verifying whether a user is authorized to access the remote system by accessing a server that is remote from the local computer system” and “processing the Hypertext Transfer Protocol command into a File Transfer Protocol command without de-encapsulation using a server that is remote from the local computer system.” The Pallman reference teaches that modular software may be utilized to acquire/retrieve source data, deliver data to a target, or to perform processing of source data (see Abstract and column 27, lines 33-54). However, the Pallman reference is silent a teaching or suggestion readable on the system of user verification that is a part of the Applicants method for controlling remote systems as is recited in Claims 1, 15 and 25. More specifically, the Pallman reference does not show or suggest: (1) verifying whether a user is authorized to access the remote system by accessing a server that is remote from the local computer system and, (2) “processing the Hypertext Transfer Protocol command into a File Transfer Protocol command without de-encapsulation using a server that is remote from the local

computer system.”

In fact, nowhere in the Pallman reference is it taught or suggested that authorization for a user to issue commands to a remote system is verified by accessing a server that is remote from a local computer system as is set forth in the Applicants' Claims. Consequently, Pallman simply does not teach what the Examiner relies upon it as teaching and does not anticipate or render obvious the embodiments of the Applicants' invention as are set forth in Claims 1, 15 and 25.

Blum et al. does not teach or suggest a modification of Pallman that would overcome the shortcomings of Pallman noted above. More specifically, the cited combination of Blum et al. and Pallman does not anticipate or render obvious a method for controlling a remote system over the Internet by executing a command through File Transfer Protocol including the steps of “verifying whether a user is authorized to access the remote system by accessing a server that is remote from the local computer system” and “processing the Hypertext Transfer Protocol command into a File Transfer Protocol command without de-encapsulation using a server that is remote from the local computer system.” Blum et al. only discloses a transparent proxy server that facilitates the establishment of data communications between devices (see Abstract). The Blum et al. reference teaches that a transparent proxy application listening on a predetermined port may receive requests in the native protocol of the request and may operate to establish the requested communication (column 3, lines 42-58). Moreover, Blum et al. discloses that it is known in the art that an “encapsulation routine” may encapsulate an FTP command within an HTTP

command and thereafter transmit the encapsulated command to a proxy server (column 1, lines

58 – 65). The server may then “strip the FTP command from the HTTP encapsulation before making a connection over the Internet in native FTP mode” (column 1, lines 58 – 67). By contrast, the Applicants’ method as recited in Claims 1, 15, and 25 requires that commands be transmitted over the Internet as Hypertext Transfer Protocol without File Transfer Protocol components and be processed into a File Transfer Protocol command and forwarded to a remote system as is set forth in the Applicants’ claims.

Moreover, nowhere in the Blum et al. reference is it taught or suggested that authorization for a user to issue commands to a remote system is verified by accessing a server that is remote from a local computer system as is set forth in the Applicants’ claims. Consequently, Blum et al. simply does not teach or suggest the embodiments of the Applicants’ invention as are set forth in Claims 1, 15 and 25. Consequently, Pallman either alone or in combination with Blum et al. does not anticipate or render obvious the embodiments of the Applicants’ invention as are set forth in Claims 1, 15 and 25.

Booth does not teach or suggest a modification of Pallman that would overcome the shortcomings of Blum and Pallman noted above. More specifically, Booth alone or in combination with Pallman and Blum does not anticipate or render obvious a method for controlling a remote system over the Internet by executing a command through File Transfer Protocol including the steps of “verifying whether a user is authorized to access the remote system by accessing a server that is remote from the local computer system” and “processing the Hypertext Transfer Protocol command into a File Transfer Protocol command without de-

encapsulation using a server that is remote from the local computer system” as is recited in Claim 1 (Claims 15 and 25 contains similar limitations).

Booth discloses a method and apparatus for compressing hypertext transfer protocol messages. The Examiner contends that Booth teaches a transmission system that employs a transmission of “Hypertext Transfer Protocol Without File Transfer Protocol” and that processes “the Hypertext Transfer Protocol into File Transfer Protocol command without de-encapsulation...”. By contrast, as discussed above, the transmissions executed as a part of the Blum system’s operation involve an encapsulation of FTP commands using an “encapsulation routine” that encapsulates an FTP command within an HTTP command and thereafter transmits the encapsulated command to a proxy server (column 1, lines 58 – 65). As disclosed in Blum, the server may then “strip the FTP command from the HTTP encapsulation before making a connection over the Internet in native FTP mode” (column 1, lines 58 – 67). Therefore the imposition of a scheme such as is disclosed by Booth (where a Hypertext Transfer Protocol command is processed into a File Transfer Protocol command without de-encapsulation) into the system of Blum that relies on the encapsulation and de-encapsulation of File transfer protocol commands would destroy an essential principle of operation of the Blum system, and thus would not be obvious to one of ordinary skill in the art.

Moreover, nowhere in the Booth reference is it taught or suggested that authorization for a user to issue commands to a remote system is verified by accessing a server that is remote from a local computer system as is set forth in Applicants’ Claims 1, 15 and 25. Consequently, Booth

either alone or in combination with Pallman and Blum et al. does not anticipate or render obvious the embodiments of the Applicants' invention as are set forth in Claims 1, 15 and 25.

Therefore, Applicants respectfully submit that Pallman, Blum et al. and Booth, either alone or in combination, do not anticipate or render obvious the present claimed invention as recited in independent Claims 1, 15 and 25 and as such, Claims 1, 15 and 25 are in condition for allowance. Accordingly, Applicants also respectfully submit that Pallman does not anticipate or render obvious the present claimed invention as is recited in Claims 3-9, 11, 13 and 14 dependent on Claim 1, Claims 16-22 and 24 dependent on Claim 15, and Claims 27-30 and 32 dependent on Claim 25, and that Claims 3-9, 11, 13 and 14, 16-22 and 24, and 27-30 and 32 respectively overcome the Examiner's basis for rejection under 35 U.S.C. 103 as being dependent on an allowable base claim.

Claims 10, 23 and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Pallman, Blum et al. and Booth and further in view of Bowman-Amuah. Bowman-Amuah only discloses a method for providing communication services over a computer network. Bowman-Amuah does not teach or suggest a modification of Pallman that would remedy the deficiencies of Pallman, Blum et al. and Booth outlined in the responses to the above noted rejections. Nowhere in the Bowman-Amuah reference is it taught or suggested that authorization for a user to issue commands to a remote system is verified by accessing a server that is remote from a local computer system as is set forth in Applicants' Claims 1, 15 and 25 (from which Claims 10, 23 and 31 depend). Consequently, the Applicants respectfully submit that the Pallman, Blum et al.,

Booth and Bowman-Amuah references, either alone or in combination, do not anticipate or render obvious the embodiments of the present invention as are set forth in Claims 10, 23 and 31.

Claim 12 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Pallman, Blum and Booth and further in view of Sridhar et al. Sridhar et al. only discloses an enhanced network communication system where client and server communications systems are coupled over a data network. However, Sridhar et al. does not teach or suggest a modification of Pallman that would remedy the deficiencies of Pallman, Blum et al. and Booth outlined in the responses to the above noted rejections. More specifically, nowhere in the Sridhar et al. reference is it taught or suggested that authorization for a user to issue commands to a remote system is verified by accessing a server that is remote from a local computer system as is set forth in Applicants' Claims 1 (from which Claim 12 depends). Consequently, Applicant respectfully submits that the Pallman, Blum, Booth and Sridhar et al. references, alone or in combination, do not anticipate or render obvious the embodiment of the present invention as is recited in Claims 12.

Conclusion

In light of the above-listed amendments and remarks, Applicants respectfully request allowance of the remaining Claims.

The Examiner is urged to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Respectfully submitted,

WAGNER, MURABITO & HAO LLP

Dated: 5/16, 2005

Reginald A. Ratliff
Reginald A. Ratliff
Registration No. 48,098
Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060